MARCH 2021
networkingplus.co.uk

NETWORKING+

Automating manufacturing

What you actually need to know and not fear

Ian Millington, adi Automation, *p7*

The path to mass-market

A strategic path to SD-WAN explained inside

Marc Bouteyre, Ekinops, *p13*

Questions & answers...

Networking+ talks life with Neil Hammerton of Natterbox

Neil Hammerton, Natterbox, *p16*

Criminals steal sensitive data on UK aid projects overseas

Cyber criminals have stolen sensitive data relating to British aid projects overseas, including details related to projects funded by a secretive national security fund.

The UK's Foreign, Commonwealth and Development Office (FCDO) and experts from the National Cyber Security Centre (NCSC), an arm of GCHQ, are investigating how a "third party" came to obtain the data, according to reports.

The FCDO has also told companies and individuals involved in pitching tenders for UK government projects that their personal data has been compromised.

An email from the FCDO said: "Some of these documents included your personal details, compromising some, or all, of the following categories: your name, work and contact details, location and nationality."

Individuals affected by the breach include those working on UK aid projects financed by the Conflict, Security and Stabilisation Fund (CSSF) - a £1bn pot of money overseen by the National Security Council. It funds projects intended to resolve conflicts and build stability overseas.

Its most recent annual report said the fund supported programmes ranging from peacekeeping in Sudan, where the UK deployed 300 personnel, to projects designed to counter terrorism and violent extremism in the Middle East and Asia.

MPs and others have in the past expressed significant concern about the lack of transparency, accountability and leadership of the CSSF.

The information commissioner's office has been informed of the breach and is being updated on the government's response.

Moreover, individuals have been advised to take steps to protect themselves online as an immediate precaution by watching out for suspicious emails, calls or text messages.

Nigel Thorpe, technical director at SecureAge, told *Networking+* that while there are few details of this data breach it, seems that stored data has been compromised. "Malware delivered by email is a likely culprit but cyberattacks through breached hardware or compromised supply chain services - such as SolarWinds, or the Accellion File Transfer Appliance - are also possibilities," Thorpe said. Faced with software shortcomings, human error and the huge complexity of an IT infrastructure, organisations need to accept that it's a case of when, not if they will get hacked." Thorpe added that cybercriminals look for sensitive, compromising or financially beneficial data - much of which is considered by organisations to be inconsequential, even if they know the location of all this information. "If all data were universally encrypted then stolen data would be useless: breached? Yes, but damaged? No," he concluded.

continued on page 2

Criminals steal sensitive data

Continued from page 1

The data theft also coincided with news that hundreds of UK companies have been compromised as part of a global campaign linked to Chinese hackers.

Cyber-security firm Eset said more than 500 email servers in the UK may have been hacked, while many companies are not aware they are victims of the attack.

"We are living in a period in which the modern world endured not just a historic pandemic, but some of the most aggressive and costly hacking events ever seen," said Ruth Schofield, UK country manager of Danish security specialist Heimdal, told Networking+. "Hospitals, schools, clinical trials, vaccine research, supply chains, technology and cybersecurity firms and government agencies were all, in some way, shape or form, hijacked by hackers. And not just with usual state-sponsored, suspect line-up from Russia, China, Iran and North Korea but newer players, who were caught hacking one another in an attempt to glean any intelligence or advantage they could in a pandemic."

Schofield added that while the origination and exact route of the CSSF breach is still unclear, "it's highly probable" that it leveraged one of the traditional vectors such as insider threat, data leakage, email threat and fraud prevention. As with every situation, prevention is better than cure and simply wishing we had been better prepared is not going to cut it," she said.

An FCDO spokesperson said: "We take data security very seriously and we are thoroughly investigating this incident." ■

Sepura's SCG22 approved for use on airwave and BDBOS networks

Sepura's SCG22 mobile radio has been approved for use by both airwave and BDBOS for use on the UK's public safety national networks.

The network approval enables public safety organisations – including police, fire and ambulance users – to deploy the SCG22 to their fleet vehicles, control rooms and associated critical communications functions.

Sepura has developed the SCG22 to meet the needs of demanding users looking for a tough and powerful TETRA mobile that can be deployed in cars, trucks, trains, boats, on motorcycles or in control rooms as part of solutions that support operations with intelligent automated features.

The device also complements the SC20 and SC21 hand-portable radios, by extending the same powerful connectivity and functionality to a mobile radio. Combining advanced connectivity through Wi-Fi and Bluetooth, the SC Series enable fast access to mission critical data, adding value to the solution.

In addition, the Wi-Fi connection supports the use of over the air programming, enabling much quicker fleet programming and management, with much less impact on fleet administrators.

Sepura said it has made the process of upgrading to the new mobile radio as simple as possible, reducing the cost of deploying maintenance staff and taking vehicles out of service for extended periods. Many of the accessories and connecting cables from the SRG3900 can be reused, and the SCG22 fits the same mounting units.

"The SCG22 is designed to support critical communications users in their everyday tasks," said Phil Woodley, Sepura's head of products – devices. "Having the same user interface and functionality as the hand portable models reduces training needs and risk of user error, while applications can be installed through Sepura AppSPACE to enhance the safety of users."

The SC radios can be used as single points of data sharing for field officers, by connecting to additional devices or data sources and sharing information over the secure TETRA network. Terence Ledger, worldwide sales director at Sepura, added: "Throughout 2020 we have seen significant demand for Sepura's solutions, with users in public safety, transport, utilities and mining turning to trusted, proven communication solutions to enable them to carry out safe and efficient operations." ■

Assured Data Protection launches new XDR Service

Assured Data Protection (ADP) has launched its eXtended Detection and Response (XDR) service, providing enterprises and MSPs with a fully automated and managed XDR solution powered by Confluera.

The service delivers XDR across multiple data streams and complements existing cloud data backup and recovery systems to provide pervasive cloud data management.

ADP already delivers enterprise-grade data backup, disaster recovery and business continuity as a service. Having signed a partnership agreement with Confluera, it has added advanced threat detection and remediation to its extensive data protection portfolio.

Simon Chappell, CEO, Assured Data Protection

The XDR service enhances enterprise data protection capabilities and integrates seamlessly with an organisation's data management infrastructure.

It can be deployed as enterprise software or as a managed service, either in the cloud or as an on-premises solution, depending on business requirements.

ADP enables businesses and MSPs to actively manage and monitor all data activity across their IT and cloud infrastructures via a single management interface.

This new XDR capability will provide more comprehensive data protection. It allows enterprise businesses and MSPs to pinpoint and track data breaches as they happen. The service will also alleviate pressure on security operations and eliminate the need for IT teams to retrospectively identify and track threats.

"We are data protection specialists so it was only natural that we would eventually provide our customers with smart threat detection and response," said Simon Chappell, CEO, Assured Data Protection. "Every day we help our customers recover data in the event of system failures, or damages to software and hardware. We're now able to extend that service by helping customers to mitigate the impact of data breaches in real-time, all under the umbrella of data protection. We're excited to share this with our customers and our MSP partners to create new data protection ecosystems that incorporate XDR." ■

BT upgrades network and connectivity for Walgreens Boots

BT has secured a new multi-year contract with Walgreens Boots Alliance (WBA) to continue as its network partner in the UK and Republic of Ireland.

Under the terms of the contract, BT will transform WBA's networking and deploy next-generation technology to improve the experience for employees and customers.

BT's network will provide faster, more responsive access to applications and data and simplify the roll out of new customer service innovations as part of WBA's digital transformation.

Joris van Oers, managing director, resources, manufacturing and logistics & Europe, BT, said: "Connectivity is central in the new digital environment WBA is creating for its customers. Our managed network will provide secure and reliable access to applications and data in the cloud and support innovation by providing agility to deploy new services faster."

Furthermore, the new, managed service will support the shift of business applications and data in the UK and Ireland to the cloud to improve the reliability and performance of connectivity in the company's stores, warehouses, distribution centres and support offices.

BT has secured a new multi-year contract with Walgreens Boots Alliance

The solution includes the transformation of voice services across Boots stores, cyber security to protect customers, colleagues and devices and extending mobile connectivity — with plans to include 5G — for service resilience and to expand capacity to support peaks in demand.

"We chose BT because we share a focus on delivering standout customer experiences," Steve Rempel, senior vice president and international chief information officer, WBA. "Our digital plans demand full visibility, control and security of applications and data crossing our network so we can join up in-store and online experiences for customers and colleagues alike." ■

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Sean McNamara
seanm@kadiumpublishing.com
Contributors: Gerry Moynihan, Ian Millington, Lukas Baur, Marc Bouteyre, Neil Hammerton

ADVERTISING & PRODUCTION:
Sales: Kathy Moynihan
kathym@kadiumpublishing.com
Production: Suzanne Thomas
suzannet@kadiumpublishing.com
Publishing director: Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by: Kadium Ltd, Image Court, IC113, 328/334 Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537

ISSN: 2052–7373

Norfolk Fire & Rescue deploys ESN-ready mobile solution

Norfolk Fire & Rescue Service has deployed an Emergency Services Network (ESN)-ready mobile data terminal (MDT) solution across its fleet of 66 vehicles, using Panasonic devices and Cradlepoint giagabit-enabled rugged LTE routers.

The fire service has deployed Panasonic Toughbook 33 tablets in the front cabs of its fire appliances as mobile data terminals (MDTs) and Cradlepoint NetCloud and IBR1700 Series routers for 4G LTE connectivity via EE, Vodafone and the forthcoming Emergency Services Network.

Panorama antennas fitted to the vehicle roofs to optimise connectivity were supplied by Westbase.io, long-term Panasonic partner and Cradlepoint distributor in Europe. MDTs are used for receiving and providing vital information on the way to an incident, such as sending status updates, risk assessment requirements, details on the occupancy of the premises and nearby hydrant locations.

The solution also creates a 100m, wireless local area network (WLAN) around the vehicles, providing firefighters with the ability to remove the MDT from the cab and take it with them during incidents. In addition, the device can then be used for continued communication with the command centre at the scene of an incident or to assist fire crews with detailed schematics of buildings or vehicles to help rescue trapped people.

Once outside of the "Wi-Fi Bubble", the Toughbook 33 has the capability to move to its own ESN Connect capable modem to continue communication if required.

NetCloud Manager, part of the Cradlepoint NetCloud Service, is now being used to manage the mobile broadband network, local Wi-Fi network and router devices, providing the visibility to monitor location, network uptime, security, and cellular reception and usage through at-a-glance dashboards. The service also enables routers to intelligently handle traffic flows across multiple cellular connections to ensure optimal performance, including over nationwide public safety networks like the ESN.

"The Panasonic device itself is great and we are yet to have a single hardware failure," said Anthony Fearn, ICT technical manager at Norfolk Fire and Rescue Service. "The Cradlepoint routers have also been rock solid. We can observe the connectivity to each vehicle and see the physical location on a map. We can see exactly how the EE and Vodafone networks are performing and we have seen a significant improvement in connectivity. A lot of the uptimes are now 100% and we have a solution ready for the switch to ESN." ■

Norfolk Fire & Rescue Service in action

Proximity expands data centre facility

Proximity Data Centres, UK regional edge colocation data centre provider, is expanding its facility in Nottingham due to rising demand in the Midlands for edge colocation capacity.

The company has given the go ahead for the multi-million-pound construction of a new 5000 sq. ft data hall which will take the Nottingham site's total net technical space to 33,000sq ft across six halls. With this, 1MW of additional IT load capacity is to be added to the facility's existing 4MW supply. The new hall is due for completion in Q3 this year and is being funded by Proximity's funding partner, Intermediate Capital Group Plc.

"Our Nottingham data centre was acquired just 12 months ago as one of our first edge locations and since that time we have experienced rapidly growing demand - from both enterprise businesses and service provider organisations," said John Hall, managing director - colocation, at Proximity Data Centres. "We're seeing growing interest from cloud, telecoms and content providers, alongside financial services companies, manufacturers and the public sector."

Hall added that "many are looking for additional scalable and low latency colocation capacity to better serve their local offices or customers" in the Midlands region. "Others are looking at colocation for the first time and want the convenience of a local and affordable high-calibre solution," Hall added. "Bringing their data closer to their users allows our customers lower latency and reduced data transit costs compared to using colocation facilities outside of the Midlands area."

In late 2020, Proximity added three new immediately available edge data centres to its UK network, in Liverpool, Chester and Coventry, joining existing sites in Nottingham, Wakefield and Bridgend. The company wants to have 20 colocation sites across the UK within the next 12 – 18 months, enabling the company to offer nationwide-wide coverage. All data centres are selected for their proximity to major conurbation areas.

Each of Proximity's data centre sites "develop renewable energy solutions, including battery storage, solar and wind power". ■

Budget 2021:tax relief for data and cloud, digital skills for SMEs

Chancellor Rishi Sunak announced a number of measures relating to the technology sector as part of the government's spring 2021 Budget, focused on areas including digital skills. He also unveiled new IT funding to improve tax collection, as well as the possibility of bringing data and cloud costs into the scope of tax relief for research and development (R&D). Sunak said investment is key to making the UK economy more productive - and improving the technology, infrastructure and skills people need in order to produce goods and services is core to that plan. Alongside the Budget, the government also released its Build back better growth plan, aimed at achieving economic recovery based on the investment pillars of infrastructure, skills and innovation.

Ideal Networks to rebrand as Trend

Ideal Networks, manufacturer of data cable, network, and CCTV test equipment, will be known as Trend Networks from March 31, 2021. In re-branding to Trend Networks, with a new tagline "Depend on Us", the company said aims to better reflect its vision, mission, goals, and position as a partner providing customers with innovation alongside dependable results, equipment, and support. The name change also consolidates the company's identity following the acquisition from Ideal Industries more than two years ago by CBPE Capital alongside the incumbent management team. "Trend Communications was a leading business with a strong reputation and a dedication to delivering industry-firsts," said Paul Walsh, CEO for Ideal Networks.

ISP Voneus brings superfast broadband to villages in County Durham

Businesses in the neighbouring villages of Ouston and Perkinsville in County Durham can now access *"superfast broadband"* thanks to the deployment of a new fibre-fed fixed wireless access (FWA) network by Voneus. Both villages now have speeds of 30-50Mbps, having previously *"struggled with patchy connections and insufficient speeds,"* with some areas only able to get a weak ADSL service. According to Voneus, the location makes it expensive to lay FTTP into this area and so the operator instead installed a fibre optic fed wireless network at the Ouston & District Social Club. The venue beams broadband southwards, to the Red Lion pub, via a high-capacity Point-to-Point link.

'China-linked group targeting Exchange'

US giant Microsoft is urging customers to download software patches after state-sponsored hackers based in China broke into some customers' copies of its software for email, contacts and calendar using multiple previously undiscovered flaws. Attackers used the vulnerabilities to hack into Microsoft Exchange Server, allowing them to break into email accounts and install malware to "facilitate long-term access to victim environments," the company said. It also released patches for the flaws in a blog about the attack. "Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks," the blog said.

Research shows data access is more critical for 53% of respondents since pandemic

Market research commissioned by Starburst and Red Hat, shows that data access has become more critical for 53% of survey respondents throughout the pandemic as analytics workloads and demands increase significantly. *The State of Data and What's Next survey conducted by independent research* firm Enterprise Management Associates, found that the imperative for faster data access is about driving business outcomes, with 35% of survey respondents looking to analyse real-time changes to risk and 36% wanting to improve growth and revenue generation through more intelligent customer engagements. The 402 respondents were located in the UK, US, Canada, France, Germany, Australia and Singapore. "Data is the lifeblood of any business trying to navigate today's digital economy," said Justin Borgman CEO of Starburst.

Npower customer accounts hacked via a credential-stuffing attack

British energy firm Npower suffered a major data breach involving hackers using stolen passwords to gain access to a large number of customer accounts.

The company had to shut down its mobile app altogether to mitigate the breach that took place February 2 and said that hackers recently carried out large-scale credential-stuffing attacks inside its mobile application to access the personal records of customers such as names, dates of birth, and addresses.

Hackers also accessed financial records such as sort codes and the last four digits of bank account numbers, and also gained access to information on whether customers preferred to be contacted by email, text, or phone call.

Adam Palmer, chief cybersecurity strategist at cybersecurity company Tenable said a data breach "is often only the start" of a series of privacy concerns for victims.

"According to Tenable Research's analysis of 730 publicly disclosed data breaches last year, 22 billion records were exposed," Palmer added. "That's a lot of information that attackers can use to further their malicious activities. The attack against the Npower app is just the most recent example of cybercriminals using previously stolen or leaked consumer data to launch additional attacks."

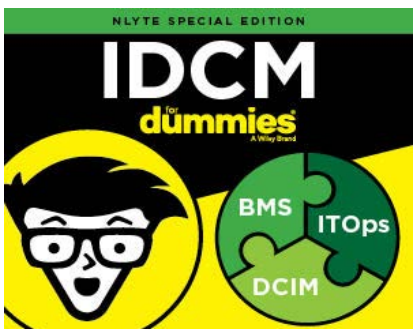
Known as 'credential stuffing', Palmer said that attackers inject large amounts of stolen passwords or IDs against other accounts with the goal that a small number will successfully allow access to the victims' accounts. "This attack is successful because many consumers use the same credentials for multiple accounts, the equivalent of using the same key for multiple locks," he said.

"These are not advanced attacks and the risk can be significantly reduced if online users use unique passwords for each account. For businesses, these attacks are also one of the reasons they must act quickly to notify consumers of a data breach so steps can be taken to change passwords or monitor accounts.

Adam Palmer, chief cybersecurity strategist at cybersecurity company Tenable said a data breach "is often only the start" of a series of privacy concerns for victims

Open book

Integrated Data Center Management for Dummies is an e-Book by nlyte explaining the importance of IDCM. Visit: *https://networkingplus.co.uk/training-events*



Word on the web...

Time for a change? By Jeremy Wastie, head of public sector sales, MLL Telecom

To read this and other opinions from industry luminaries, visit www.networkingplus.co.uk

TREND NETWORKS

Depend On Us

Pressure on networks is increasing and downtime is expensive.

Fix it fast with SignalTEK 10G.

SignalTEK 10G

10G Ethernet Troubleshooter and Bandwidth Tester

SignalTEK 10G measures the maximum network bandwidth available, identifies bottlenecks and discovers opportunities to increase bandwidth without replacing expensive data cabling.

Key Features

- **Determine max bandwidth** up to 10 Gb/s
- **Verify Multi-Gig upgrades** on existing cabling
- **Pass/Fail to 1/2.5/5/10Gb** IEEE standards
- **Eliminate PoE guesswork** up to 90W
- **Pinpoint network issues** with 72h event log
- **Copper and fibre interfaces** up to 10Gb
- **Prove performance** with PDF reporting

TREND AnyWARE CLOUD

For a 20 minute demo or to trade-in your old SignalTEK CT/NT please call **(0)1925 428 380** or visit **www.trend-networks.com**

Putting the human at the heart of HR cybersecurity culture

Andrea Babbs, UK general manager, VIPRE SafeSend, discusses what the new remote way of working means long-term for HR departments

The pandemic has forced businesses to revise their working processes; from shifting overnight to a remote working model and operating in a challenging economic climate, many companies were unprepared for these transitions. However, these changes highlight the important role of Human Resource departments in communicating and responding to the necessary adjustments and helping employees through the process.

As HR departments reconsider how they strengthen their organisations, front and centre to that shift needs to be IT security, underpinned by digital tools and a cyber-aware culture. With a 31% increase in cyberattacks during the height of the pandemic, reinforcing cybersecurity should be at the top of HR's agenda.

Managing dispersed teams

With decentralised workforces, there is extra pressure for HR teams to effectively manage their employees. As the 'Bring Your Own Device' phenomenon creates a security concern due to the lack of consistent security software, as well as the pressure of staff feeling the need to work harder, faster and for longer, it's no surprise that mistakes will be made.

Recent research has found that more than half of businesses believe working from home has made employees more likely to circumvent security protocols, such as failing to change passwords. Inappropriate use of business equipment might also be an issue, including browsing unsuitable websites, which must be managed with the appropriate controls, such as blocking access to websites that could drain productivity.

With the combination of untrained employees and creative hackers, the challenges of maintaining security are evident. However, by implementing the correct security solutions across all employees' devices, these risks can be mitigated.

Protecting employee data

As well as managing their employees, Human Resource departments have a vital role to play in keeping information safe. HR managers deal with sensitive information daily, including health records, financial information and employee's CVs – a gold mine for cyber hackers.

Additionally, the personal information stored within HR must comply with General Data Protection Regulation (GDPR), meaning that if this data was to be stolen by cyber hackers, the consequences could be devastating. New results found there was a 19% increase in the number of breach notifications, from 287 to 331 breach notifications per day.

Email is a key communication channel for HR managers to share this personal information – which is a risk in itself. The repetitive nature of email usage means that users can often forget that without the right protocols in place, email can be a window to serious cybersecurity breaches. However, luckily there are digital tools available that offer that critical second check.

Heightened email security

Throughout the pandemic, there has been an increase in the number of attacks using COVID-19 as a lure to vulnerable employees. Also, email addresses of those in HR are typically made publicly available for job applications, which is also an open opportunity for malicious attachments, disguised as CVs perhaps, to be sent.

HR teams can support employees to avoid not only making mistakes, but also be wary of potential email attacks, by deploying innovative technology. Digital tools, such as VIPRE's SafeSend, provide a simple safety check, prompting the user prior to sending an email to confirm it is correct – going to who it should, with the right information. Such tools can also help in the event of a phishing attack by highlighting external email addresses which try to look like they have come from someone internally.

SAT programmes

Employees themselves are often the number one gateway for cyber-attacks. According to CISOs, human error has been the biggest cybersecurity challenge during the COVID-19 pandemic. It's more crucial than ever for Human Resources to reinforce the need for a strong cyber aware culture, and this can be done through security awareness training programmes.

HR teams are often involved in implementing the right programme to suit the needs of their workforce. Key considerations should be around the frequency of training, how engaging the training is and the reports available to show improvement over time.

As well as implementing training for their employees, HR departments should also receive their own continuous training, which focuses on mitigating the legal, financial and reputational risks that come with cyber-attacks. Not only will training mean employees are aware of how personal data should be handled, but it will also increase accountability.

Conclusion

Covid-19 has presented new challenges to human resources teams but has also changed the future of the workplace. However, among these many transitions, cybersecurity must remain a priority. As threats continue to become more advanced and target those who are vulnerable, it is the job of HR to act now and deploy a layered approach to cybersecurity in order to keep sensitive data safe. Above all, for this secure infrastructure to be effective, employees must understand their responsibility when it comes to cybersecurity by taking a proactive role in keeping business information safe.

Monitoring from home: 3 things to watch in your IT network

The move towards remote work has been nothing short of tremendous. In most cases, IT departments all over the world worked miracles to get it all working. But, as any IT administrator will tell you: the battle is not over. Because it's one thing to get this all up and running, but another thing to keep it up and running.

Part of the challenge for sysadmins right now is that **not only are their users logging in remotely, but so are they.** This means that they are far away from the physical server room in their headquarters. So just how do they ensure that everything is running as it should?

The answer to this question is the same as when everyone is working in the office: network monitoring. And, if you are using PRTG Network Monitor, here are three things you can (and need to!) keep an eye on when working remotely.

1. Bandwidth

Bandwidth remains key to how effectively users can access and use services and applications. Low bandwidth could result in all kinds of detrimental issues for remote work. A stuttering connection to a video conference will make meetings a nightmare, or a slow connection to a service like Microsoft 365 or Confluence could make quick tasks take twice as long. In short, bandwidth is probably the most crucial element to monitor.

Bandwidth is a tricky problem because there are now so many variables that could affect a user's connection to services—and many of these variables are outside of your control. First, there's the user's wireless network at home, which might have countless devices connected to it right now. Then there's the user's connection to the Internet itself. This is almost impossible to monitor.

However, you can actively monitor what is going in your organization's network– even if you are not physically on premises. The trick here is to monitor potential problem spots in the network so that you know when there is traffic congestion – before your users tell you. There are various ways you can do this with PRTG Network Monitor:

- **Use SNMP sensors:** Bandwidth monitoring with SNMP will tell you the amount of traffic, over time, on each port.
- **Use Flow sensors:** PRTG lets you use Flow protocols to identify the devices generating the most traffic, the connections using the most traffic in your network, and so on.
- **Use the Packet Sniffer sensor:** analyze traffic in your network and produce top lists.

2. The VPN

If your workforce logs in to their environment through a Virtual Private Network, you probably now have dozens or even hundreds of remote workers connected. Of course this means you need to be consistently sure that your VPN is functional.

The key aspects to consider with VPN are the traffic in and out of the VPN, and the number of connections. Slow traffic might indicate a potential problem, and knowing the number of currently connected users can help with troubleshooting and diagnosis.

PRTG uses Simple Network Management Protocol (SNMP) for its VPN monitoring. If your VPN environment is based on Cisco ASA or SonicWall devices, PRTG offers a number of default sensors that use SNMP to monitor the VPN traffic, users, and connections of those solutions. If you use another VPN option, you can use PRTG user-defined SNMP sensors. Manufacturers such as Juniper and Fortigate provide MIB files that you can incorporate into PRTG with the SNMP Library Sensor.

3. Teleconferencing tools

There's no doubt that the glue holding virtual teams together right now is online video meetings. Teleconferencing tools, like Microsoft Teams, Zoom, and others, are the only way that teams can continue working as...well, teams. So of course, these need to be up and running.

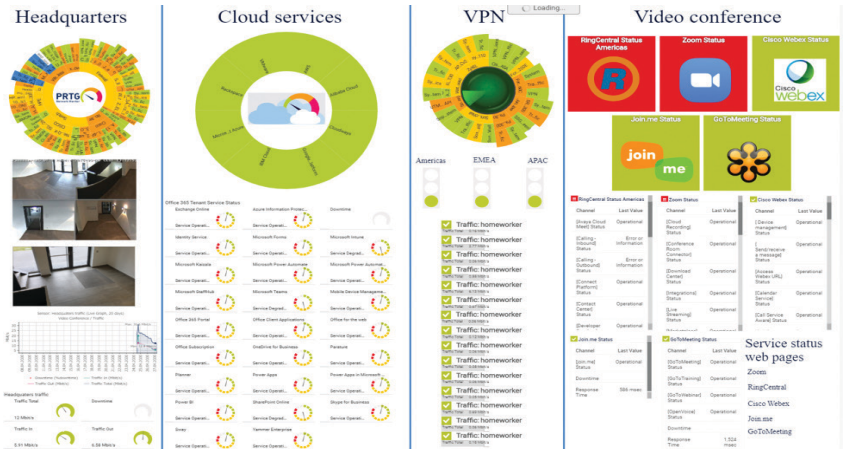
While PRTG doesn't necessarily offer a direct way to keep an eye on these tools, there is a way to do it indirectly. Most services offer either an API or a Website for users to check on the availability of the service. For example: Zoom offers this service status, along with details of an API to query the status. You can use this information in conjunction with the REST Custom sensor in PRTG to get notifications when the service you make use of is down. We'll be posting exactly how to do this in a future post.

Monitoring from home with PRTG

Of course, there are also countless other things to keep track on; the above are just some of the more important ones when a large part of your users are working remotely. PRTG helps you with all of it.

The way that PRTG works is that you install a PRTG server in your environment, which then collects data from your devices infrastructure and network. You can **create dashboards and access them from anywhere**—even from home

Here's an example of what such a dashboard could look like: You can also configure alerts and notifications to be sent to your mobile device, so you are always aware when something fails without continuously having to check it. If you want PRTG to help you out while working remotely, give it a try by downloading our fully featured 30-day trial here.



Automating manufacturing resiliency

Ian Millington, managing director, adi Automation

Automation is causing seismic shifts across many industries, as the adoption of intelligent technology promises to transform the way we live and work.

Before Covid-19 arrived on the scene and took the world by surprise, a business' ability to adapt and respond to marketplace changes was strong indicator of its industry success. Fast forward to today, and without this kind of business mobility, manufacturers expose themselves to a ruthless economic climate, whereby manufacturers across the world are having to down tools and shut up shop to such an extent that they could be doing it for the last time.

Supply chains have been particularly exposed at this point in time, as manufacturing resiliency, flexibility and scalability is put into perspective with increased food demands, data centre needs and medical responsibility.

Business owners have had to learn the hard way that a dependency on human labour and access to physical space makes it vulnerable to disruption. So with the manufacturing industry looking to fight back against the virus, we'd argue that now is the time for automation to take its place in achieving a highly cohesive, resilient and responsive manufacturing ecosystem.

Automating fear

It's no secret that manufacturers have long intimated a desire to automate systems, yet this has been juxtaposed by an ingrained resistance for decades. Of course, the cost of implementation and a fear for the loss of human jobs has been well publicised over the years, so when you consider an economic climate whereby job safety is at a premium, it's a little wonder bosses have further retrenched into old habits.

Low cost at a reasonable rate of quality has become the norm for the past 20 years, which has often resulted in manufacturers looking overseas to secure cheap labour, land and shipping infrastructure. But with the global pandemic rattling this old school supply chain in a massive way, now is the time for manufacturers to step up and act differently if they want to not only survive but thrive in the years ahead.

Robot and human efficiency

Firstly, there's solid evidence out there that automation doesn't really lead to a loss of human jobs. Think of one of the oldest industries out there – farming. While it is true that in the early 20th century, there were over 10m farmers in the US alone, compared to one million today, it is also true that this decline was accompanied by new technology, which created jobs in the service, blue collar and white-collar industries. In reality, automation creates jobs in new digital based roles that are expected to have a global economic impact of over £11trn by 2030.

Remote guidance

Capital expenditure has been in heavy retreat during the pandemic, so it is of some relief that by deploying robots to automate many of the mundane, repetitive tasks associated with manufacturing processes, firms can shift their spending from capital to operating expenses, minimising both cost and risk.

One of the huge benefits that has enabled many factories to continue operations as normal, amidst social distancing guidelines, is remote working practices. At adi, we've seen the benefit of this in our partnership with Rockwell Automation and its ThinManager production platform. Delivering centralised data management via a single server-based technology, manufacturers are able to shield themselves from costly periods of downtime and production outages.

Understanding this further, take for example how manufacturing environments can be quite inhospitable to electronics such as computers. A typical PC may breakdown inside two to five years depending on conditions. If you had 20 PC stations in one plant, that could result in a massive outage or loss of data to your business taking approximately eight hours to fix at best. That's one outage potentially every two months.

ThinManager utilises Thin Clients instead of bulky PCs connected to screens on the production environment. With no moving parts, thin clients are less prone to overheating and breakdown, while they can also operate as 'plug and play' devices, meaning any downtime is minimal. The ease of installation means extra screens can be easily installed for social distancing of personnel.

Similar applications can be applied for remote monitoring systems, allowing personnel to access plant data in a variety of simple to use and graphical formats, from anywhere using equipment such as laptops, tablets or mobile phones. Data can be used and updated to maximise production whilst being away from the manufacturing environment. Remote access and monitoring is therefore transforming production sectors as diverse as food and beverage, chemical and general manufacturing.

Companies are looking for ever more innovative ways to operate efficiently with less production floor operatives being available. Automation is just one of a number of technologies which can be applied to existing facilities to improve efficiencies through use of data.

By acting now, manufacturers that can set the stage for the next wave of industrial transformation and futureproof themselves against manufacturing's next inevitable wave of disruption.

ESN health check

The ESN is something we can't live without, but an unforeseen pandemic and delayed upgrade have caused problems. Robert Shepherd examines the network

If you consider all the networks or platforms that form the backbone of any nations' methods of communication, you'd have a thankless task finding one that's more important that one adopted by the police, fire and ambulance services. Known on these shores as the emergency services network (ESN), it's what keeps the country on its feet and is something we have all used or will have to use at some point in our lives.

However, like any other network, the ESN needs regular maintenance, a need not to be overused/abused by time-wasters and prank callers, new and better technology and of course, cold hard cash to fund it all. The UK has certainly had its challenges with some, if not all of the above.

Nothing put the emergency services under the spotlight over the last 12 months (and counting) like the pandemic. The demand for hospital services caused by the rampant coronavirus has put ambulance staff in England under "unprecedented pressure", with handover delays on a scale not seen before.

That, of course, has put extra strain on the emergency services and so the nation's Emergency Services Network (ESN) has had to deal with unprecedented levels of traffic.

Add to that a raft of protests across the country in which all three emergency services were deployed, the ESN is under constant strain. Of course, the situation wasn't helped in September last year when permanent secretary for the UK Home Office, Matthew Rycroft, informed the Public Accounts Committee (PAC) that the new over budget 4G based ESN is now unlikely to completely take over from the existing

"This would provide considerable benefits over ageing TETRA infrastructure, without compromising on strong features such as high availability and security"

Nick Koiza, head of the security business, Plextek

platform until early 2024 or late 2025. Previously it was due by December 2022.

At present the emergency services interface via the Motorola-owned Airwave network, which is believed to cost the UK around £3bn and harnesses the TETRA (Terrestrial Trunked Radio) network technology.

"We have had a reset and the reset is not just about technology," Rycroft said at the time. "It is also about mindset, and the mindset reset is to put the users at the heart of this. That does take a little bit longer, but I think it is time well spent in order to get a programme that they can support, and so that's what we are doing. In terms of the dates, the absolute latest that we could turn Airwave off is 2025, and what we are seeking to do is to accelerate that date so that we can turn it off by the beginning of 2024. If we could turn it off even sooner than that, then obviously we can, but I don't want to give a date which then doesn't get met."

You'd be forgiven for thinking that all makes for very grim reading. However, things are moving along.

In the autumn of 2020, mobile operator EE, which won the contract to construct new sites and to develop a new core for the ESN, said its job is nearly done. It has built circa 1,000 new masts, upgraded 19,000 existing locations and is deploying long-range 800MHz spectrum to deliver widespread coverage. The new core will mean the network will be able to prioritise ESN traffic when required.

Then, just a few weeks ago, in the latest testing phase for the ESN, project with the Home Office, mission critical comms specialist Frequentis successfully demonstrated the additional voice and data feature set. The Emergency Services Mobile Communications Programme (ESMCP) is delivering the new ESN critical communication system, which will replace the current TETRA-based Airwave system with a new LTE-Mission Critical Services (LTE-MCx) 3GPP based radio communication system in Great Britain.

This means ESN will transmit fast, safe and secure voice, video and data across the 4G network and give first responders immediate access to life-saving data, images and information in live situations and emergencies on the frontline.

"Testing this time included group call, private call (in/out), ambient listening, status message, emergency calls, text messages and broadcast, all of which were successful thanks to the hard work and dedication of the teams," says Andy Madge, managing director, Frequentis UK. "In addition, we will be delivering functionality to support interworking between existing Airwave and ESN to provide a smooth transition for our customers as they move to the ESN network, allowing both networks to be

"The short and honest answer is that we simply don't know yet, but for sure we'll see dramatic changes once 5G becomes a reality"

Tony Gray, chief executive, TCCA

used in parallel. We are pleased to be able to adapt LifeX to fit the needs of ESN in order to further support emergency services operators in their challenging role."

Another long-time supplier of critical comms equipment is Sepura, which not only provides complete communication solutions to all emergency services, including larger organisations such as police, ambulance and fire teams, but also counter-terror, military police, border and specialist operation teams, as well as local government organisations. "Our solutions are also used by rescue and other emergency response teams, as well as by other mission critical users, primarily transport, utilities, airport and oil and gas providers," says Terence Ledger, worldwide sales director, Sepura. "Our communications solutions join the control room with field operators, enabling improved situational awareness and improved operational outcomes."

While the emergency services do, thankfully, have the very latest in technology to help essential and key workers carry out their jobs to the best of their ability, Ledger says all kit,

both hardware and software, are constantly under review, to keep in line with best practice and to match evolving operations. "This is particularly the case with software which can be designed around an organisation's specific needs and can be quickly and easily updated when necessary," he continues. "Before new products or software are accepted, they will go through rigorous testing both by the manufacturer and the end user, to ensure their reliability and suitability for the task. However, user organisation often refresh their entire radio stock together, to ensure identical user interface and programming solutions for all users. For this reason and given TETRA radios' well-earned reputation for robustness and reliability, radio fleets are often in service for over five years."

Ledger warns that this "is likely to be a significant obstacle to adoption of broadband devices for mission critical devices by large organisations",, because of the reliance on consumer-derived components, the devices would need to be updated much more regularly. "The cost for this across an organisation, when also tying in retraining, infrastructure upgrades and testing periods, is arguably currently prohibitive," he says.

US firm Rajant supplies its proprietary Kinetic Mesh wireless networking technology to police forces in the UK. This network technology provides secure, resilient CCTV coverage in areas where no fixed network exists.

"One of the police forces that we have permission to identify is Thames Valley Police due to the activities associated with Prince Harry and Meghan Markle's wedding," says Chris Mason, Rajant VP of sales EMEA.

"A significant requirement for work with UK Police Forces is to provide secure wireless networking. One key aspect of Rajant's technology capabilities is the multiple encryption levels built into every network node called BreadCrumbs. This ensures that demanding users such as the Police can implement security across the Rajant wireless infrastructure. As a result, there have been no security issues when deploying."

MLL Telecom also works with the emergency services. As well as the Scottish Fire & Rescue Service, it also provides services to Police, Fire and Ambulance services in the East Midlands, Herefordshire and Norfolk & Suffolk. These include

a mixture of private circuits, managed MPLS wide area networks, SD-WAN overlays, SIP voice services, internet connectivity and managed security services.

"One area we have seen increase in emergency services in the last 12 months is the demand for private circuits and wires-only WAN connectivity, to support the use of customer-managed SD WAN networks," says

Ross Duke, technical director at MLL Telecom. Duke says that when it comes to security, maintaining the security and integrity of personally identifiable information continues to be the biggest concern across all areas of emergency services. "This was highlighted with the Wannacry ransomware attack on the NHS in 2017 and remains one of the widest impacting attacks we have seen," he adds. "The most effective way of dealing with this and other threats is ensuring suitable processes are implemented effectively and that staff are appropriately trained in line with NCSC guidance.

As we look to the future, the fifth-generation technology, better-known as 5G is being rolled out across the country and is expected to be a major "game-changer" for a number of sectors.

There are challenges associated with 5G deployment, of course, not to mention a number of detractors. This technology requires three times as many base stations as LTE, due to higher frequencies. In addition, there is typically a threefold power consumption increase for a 5G base station. Then, factor in that initial investment required for a 5G base station is several times more than that needed for an LTE unit, which could prove cost prohibitive in the case of privately owned and managed 5G networks.

Tony Gray, chief executive of The Critical Communications Association (TCCA), a membership organisation, which represents all standard mobile critical comms tech, says

5G technology will be a key element for IoT - or the "interconnection of everything" - since it will allow billions of devices to be connected simultaneously. "This will be one outcome of the significant improvements 5G will deliver in mobile coverage, capacity and time delay reduction, and can be expected to take society as a whole far beyond the current realms of smartphones and 4G," he adds. " But how will this virtual ubiquity of ultra-fast, low latency communications and interconnected devices impact on critical communications and the work of emergency services / first responders? The short and honest answer is that we simply don't know yet, but for sure we'll see dramatic changes once 5G becomes a reality. Innovators can begin to bring to market new ideas and working practices through applications including, but by no means limited to, Artificial Intelligence (AI), Virtual Reality (VR) and the likes."

Ledger says 5G provides an exciting opportunity for commercial users to have access to more business-critical data to support their daily operations, but critically 5G is an extension of 4G and mission critical operators are still waiting for standardisation to really happen for mission critical broadband.

"For mission critical users – primarily those in the emergency services and those protecting critical national infrastructure, the most critical aspect of mission critical comms is voice," he adds. "At present 5G fails to provide mission critical levels of coverage, encryption and data security. In addition, the industry has not agreed standards to allow interoperability across multiple manufacturers. Therefore in the immediate short term, it is unlikely that many will move away from the trusted TETRA or other mission critical platforms. In time, when 5G has been regulated, tested and approved, there are exciting opportunities to join together mission critical voice and data solutions."

Nick Koiza, head of security business at Plextek, says that as the critical communications industry gradually transitions, "we are expecting to see it complement or replace highly- reliable" and secure TETRA (2G) networks with LTE (4G) technologies.

"Nationwide LTE systems for public safety are proceeding with the roll-out of the ESN in the UK," he says. "The 3GPP community has developed a set of standards for Mission Critical (MC) functions, such as Push-to-Talk (MC PTT), data (MC Data) and video (MC Video), hopefully delivering on an expectation for LTE data speeds and enhanced capacity. This would provide considerable benefits over aging TETRA infrastructure, without compromising on strong features such as high availability and security – both of which we have grown accustomed to with well-proven digital Private Mobile Radio (PMR) technology."

For Duke, the emergence of 5G is an interesting topic. He believes that as a technology, with the bandwidth and performance (latency) it can offer, it has the potential to replace fixed line connectivity in many situations.

"However, this is greatly dependant on the way the mobile operators implement and make available their service offerings," he warns "From that perspective it's very early days, and we're really seeing 5G today being used as a higher-bandwidth alternative to existing 4G offerings. Ask me again in 18 months." ■

"The cost for this across an organisation, when also tying in retraining, infrastructure upgrades and testing periods, is arguably currently prohibitive"

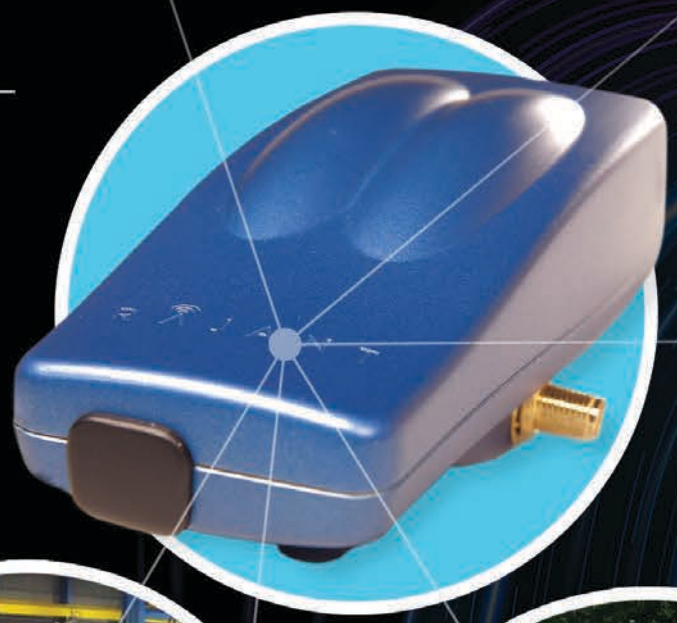
Terence Ledger, worldwide sales director, Sepura

Just like today's industrial leaders, Rajant's network is

Smart. Autonomous. Always moving.

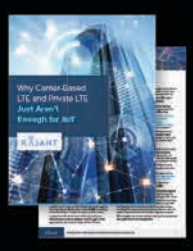
Rajant Kinetic Mesh® is the only wireless network to power the non-stop performance of next-gen applications—from real-time monitoring to robotics and AI.

- Works peer-to-peer to maintain **hundreds of connections simultaneously for 'never break' mobility**
- Intelligently self-optimizes to **change in real-time, ensuring mission-critical reliability**
- The *only* network to enable **machine-to-machine communications required for autonomy**
- Provides **Industrial Wi-Fi for extended Wi-Fi connections** in challenging environments



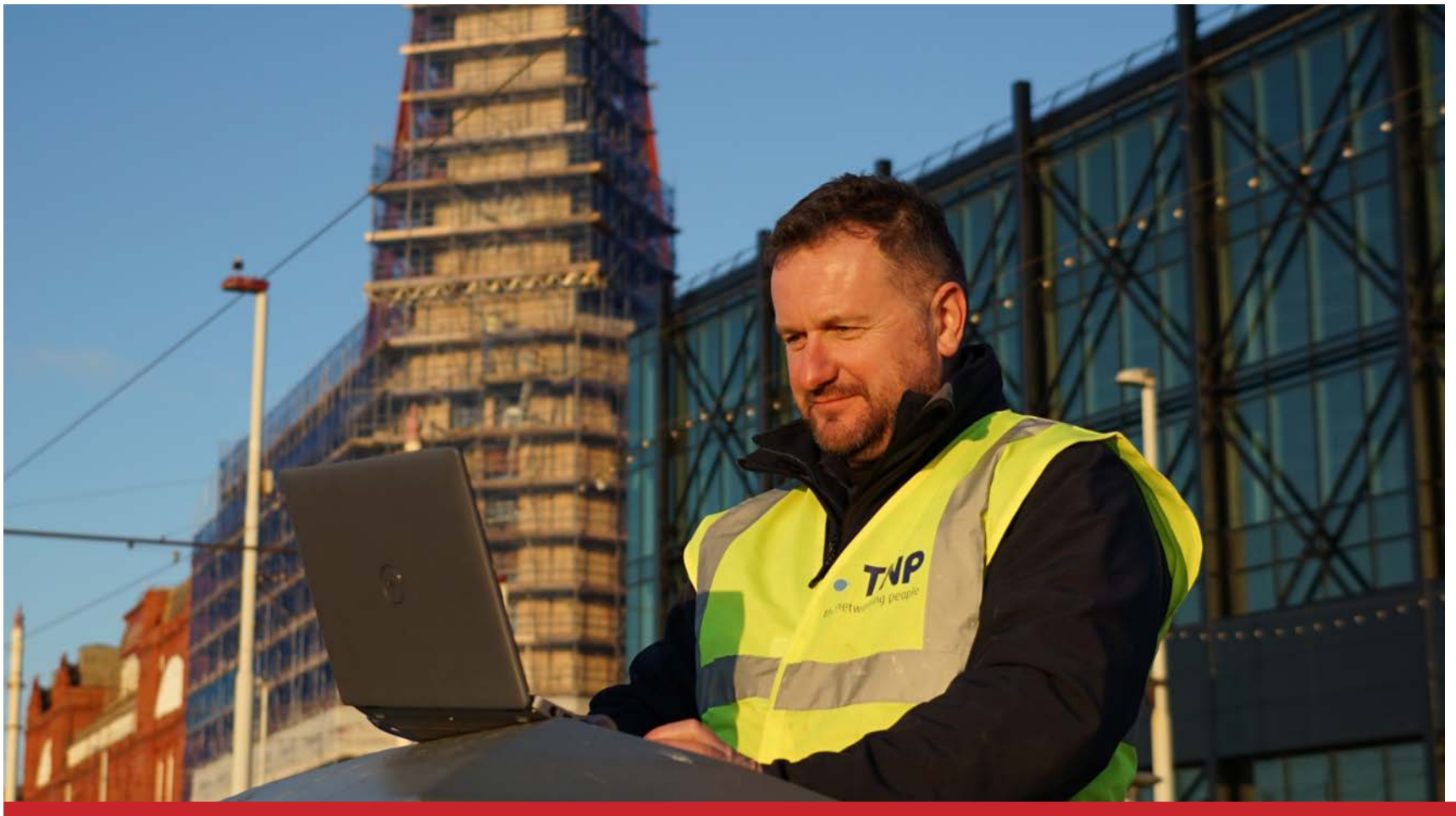
*IF IT'S **MOVING**, IT'S RAJANT.*

*Industrial Wireless Networks **Unleashed.***



Download our **"Why Carrier-based LTE and Private LTE Just Aren't Enough for IIoT"** white paper at **rajant.com/networkingplus**

RAJANT



Blackpool leads UK in completing transformational LFFN Project

Famous English seaside resort leads the UK in the way the authority has managed the rollout and got it fully up and running, thanks mainly to the strategic relationship with TNP

The foresight and strategic planning of the authority meant it had already begun the digital transformation of the town before it secured funding of £3.1m from the LFFN programme run by the Department for Digital, Culture, Media and Sport (DCMS).

TNP (The Networking People) has worked with Blackpool since 2012 and that early consultancy work and construction of high-capacity digital connectivity based on a full fibre network laid the foundations for a new digital integrated-hybrid network infrastructure created and owned by the local authority.

The partnership enabled the Council to procure the LFFN infrastructure quickly, efficiently and cost effectively, using transparent 'open book' contracts agreed with TNP that guaranteed best value at every stage of the network procurement, implementation and support lifecycle.

Tony Doyle, Blackpool's head of ICT was the project lead with support from his department and the wider development team in the Council. He explains: "Blackpool Council would have found it difficult to achieve their objectives within a two-year timescale without the long-term innovative partnership with TNP. That partnership has enabled the creation of the integrated-hybrid network, built on time and to budget through access to the highest level of network professionals in the UK."

The LFFN rollout has now been integrated into the hybrid network while maintaining the Council's total access, control and visibility of the digital infrastructure in the town, as well as sharing spare capacity in the network with an innovative broadband co-operative.

Blackpool Council already owned and operated a diverse, resilient hybrid telecoms network across its area. It incorporated a number of key technology elements including local telephone exchange assets, regulated fibre services (from Openreach) and unregulated fibre services (from alternative providers such as Virgin Media).

A comprehensive dark fibre network spanned the town centre and the 20km coastal tramway from the southern boundary to the northern end of the coast and the neighbouring authority of Wyre Council at Fleetwood. The tramway fibre was completed early in 2018 under a 'dig once' model that allowed upgrading of the tram system SCADA network to assist in the funding of a fibre communications infrastructure.

Extending, augmenting and maximising the existing network and tramway ducting meant Blackpool Council could increase connectivity to its buildings and assets, those of the neighbouring authority and other public sector partners, plus stimulate business growth by enabling high-capacity digital connectivity.

Integration with the Council's owned-infrastructure delivers connectivity to all its existing buildings, offices and schools and allows the infrastructure to be harnessed, extended and upgraded to benefit local business and the residential and guest economies. Gigabit connection vouchers are being used to increase business take-up.

At the heart of the pre-LFFN network were two highly resilient data centres with dark fibre. The newest purpose-built data centre constructed in 2014 offers co-location space currently to other public sector customers with sufficient capacity to support new co-operative customers and enhance the Full Fibre infrastructure.

The data centres were also connected via a high-speed resilient ring to Blackpool Tower for microwave radio links and by fibre to the Openreach Blackpool Central Telephone Exchange and small surrounding exchanges.

Blackpool Council successfully designed, implemented and managed a network consisting of dark fibre, telephone exchange assets and rented fibre/copper circuits that delivered connectivity to around 150 locations across the town. The dark fibre tramway network now incorporates 110 tramstops/breakout points/ Points of Presence (PoPs) which cross the carriageway and are in optimised locations to take the network inland.

These PoP cabinets provide interconnection facilities for third party fibre and ISP providers to utilise spare capacity and interconnect with the fibre infrastructure at speeds of 1Gb/s and 10Gb/s efficiently and securely, ensuring that the Council core network is not compromised.

Enabling the infrastructure for asset reuse comprised of installing additional node points that allow for "meet me" locations for third party providers such as ISPs and telecoms carriers, thus giving access to backhaul facilities and point to point high-capacity fibre.

To maximise the capacity on the Council's original digital infrastructure and new LFFN, TNP has employed wavelength division multiplexing (WDM) that combines multiple signals on laser beams at various wavelengths for transmission along fibre optic cables. This allows flexibility and capacity above that offered by a basic and passive fibre optic technology.

Blackpool has an integrated telecommunications network that it owns and is operated under a partnership model with a communications provider that has no commercial interest or ownership of the infrastructure.

As Blackpool Council's external network enablement consultancy partner TNP provided technical design authority, implementation, project management and ongoing support assistance - fully integrating all aspects of the project.

The extended LFFN network is wholly owned by Blackpool Council with TNP simply delivering designated communications provider functions, ongoing network management/billing support plus options for first, second- and third-line support (including training for Council IT staff members).

All network hardware, components and cabling are owned by the Council with TNP using its 'communication provider' status to deliver the necessary relationships with other network operators, BT OpenReach and Virgin Media. ■

Outstanding in his field: minister invited to work from pastures new

The Scottish government minister responsible for broadband was invited to work from a field by angry locals to see how he could handle 'remote working' and sample 'real life'

Furious Highlanders blighted by snail speed internet in a rural community have set up an office in a cow field – and invited the man responsible for the nation's broadband to work from it for a day.

Angry locals in a Moray beauty spot dreamt up the stunt after being brushed off by Paul Wheelhouse, the Scottish Government's Minister for Energy, Connectivity and the Islands.

Now they have set up the ultimate "remote office" – a workplace in a field in rural Finderne, near Forres, and challenged the SNP Minister to sample the realities of rural broadband for himself.

Pery Zakeri is the development manager of the Finderne Development Trust, which has been tirelessly working to bring fast broadband to Finderne since June 2019. The group is angry about Scottish government delays in providing vouchers to help Scots improve their web access.

"Working from a desk in a field in the heart of our rural community will soon let Mr Wheelhouse get a taste of the everyday reality for those trying to run a business or home school kids in this part of the world," she says.

Zakeri says the community wants to show Wheelhouse "that you can have everything you need for a workplace or home office – but in 2021 it's pretty much worthless without a functioning broadband connection."

Families and businesses covered by the Finderne Development Trust have faced years of frustration with internet connection speeds, worsened by the pressures of the Coronavirus lockdowns.

Initially they attempted to pursue a Community Fibre Partnership and pinned their hopes on getting superfast fibre connections for the 498 properties in the area. However, those dreams were dashed when the door was slammed shut by Openreach in mid-December.

Initially they attempted to pursue a Community Fibre Partnership and pinned their hopes on getting superfast fibre connections for the 498 properties in the area

Now the community has all of its hopes pinned on Mr Wheelhouse's flagship R100 – Reaching 100% programme, which promises to deliver 30 Megabits per second (Mbps) to every home and business in Scotland by the end of 2021.

However, the R100 programme has been hit by a series of delays and, as Finderne residents have been told that it could take between 4-5 years to be delivered, the community claims the Government has fumbled the rollout of interim support vouchers.

The Trust claims those £400 vouchers would help families and businesses pay for short term solutions to help them achieve faster connectivity until R100 is delivered. For most, that would simply mean offsetting the cost of slightly faster mobile connections.

But the interim vouchers will not be made available until delivery of R100 begins later this year – meaning further agonising delays for Finderne and other affected communities across Scotland. ■

The path to mass-market for SD-WAN

Marc Bouteyre, senior product line manager, SD-WAN, Ekinops

Enterprise IT has been putting more and more pressure on networks, demanding significant and ongoing increases in performance and efficiency. To keep up, SD-WAN has emerged as a compelling solution capable of evolving conventional networks quickly to meet these demands.

Yet although SD-WAN offers a huge amount of value – from greater bandwidth efficiency and programmability to a seamless on-ramp to the cloud and, ultimately, lower costs – the current market can at best be described as inconsistent. For SD-WAN to reach its full potential, it is crucial that the technology becomes part of a healthy and managed evolution of existing networks, instead of a hasty, complex and costly revolution.

Deployment challenges and costs have consistently been barriers for businesses that would otherwise move forward with SD-WAN. In theory, SD-WAN can boost SME network capacity to meet their increasing demand for cloud-based, digital services. In reality, the number of technical, commercial and strategic challenges that come with SD-WAN have kept the technology stubbornly out of reach.

Moreover, today's SD-WAN vendor landscape is complex and crowded, with competing players, disjointed approaches and an overwhelming number of options, mainly comprised of expensive off-the-shelf solutions from dominant vendors. So far, available options that don't rely on installing an expensive, dedicated SD-WAN appliance from a major vendor, have been limited.

Smaller enterprise sites and SME customers, in particular, are already contending with legacy systems migration and so struggle to to create a commercially viable business case to justify a complex and expensive multi-vendor DIY approach. Many also lack the in-house IT skills and resources needed to deliver a solution themselves.

All these factors mean that, despite SD-WAN's rapid growth and considerable traction, it has yet to break into the mass-market. For that to happen, the market needs to evolve beyond hype and early adoption to become more accessible to SMEs and smaller enterprise sites, who are battling to keep pace with ongoing digitalisation.

Of course, implementing network upgrades to a 'live' infrastructure is always challenging and most enterprises are reluctant to shoulder the responsibility or to sacrifice their legacy services. In fact, no enterprise is asking to get rid of MPLS altogether, not least because leveraging existing assets is significantly more cost-effective than replacing everything. Rather, they want greater agility and control over their application traffic management and cloud access, while keeping costs down.

This is where service providers can add real value. The emergence of DIY SD-WAN has led to increased competition, with many service providers struggling to keep hold of their place in the market.

There is a real opportunity for operators to expand relationships and tap into new revenues by offering SD-WAN as an additional managed service. After all, existing and proven carrier-grade legacy systems – plus corresponding business models of service providers – simply need some fine adjustments.

A managed SD-WAN solution takes the pressure off for enterprises, removing the need to get accustomed to new systems and technologies. By not only offering a more flexible SD-WAN solution, but taking on the service management, service providers can play this crucial network management role for their customers.

Offering SD-WAN as a managed service also allows service providers to pivot their focus on enhancing existing access infrastructure. By adding SD-WAN as a virtualised service to their product offering, service providers can simultaneously cater to businesses' other connectivity requirements while upselling new services.

Moreover, integrating SD-WAN into the core portfolio of carrier-grade legacy services allows end-customers to rely on their existing solutions while 'switching on' additional capacity, automation, and application management as and when needed. This opens the door for capacity projections, which allows customers to stop buying by-default from the big brands and paying for more than is required.

Service providers that can strike the balance between offering SMEs and smaller enterprises a robust, secure managed service that avoids network disruption and eases deployment complexity, while enabling them to define their own application prioritisation and performance objectives, will create a win-win situation. With existing infrastructure, service providers can deliver more competitive pricing models while offering first class services.

By offering customers flexible, tailored and cost-effective solutions that support legacy technology, service providers can reach customers who would otherwise struggle to make the business case for the technology. This allows them to not only get back in the SD-WAN race, but to get ahead of the competition posed by new entrants.

This strategic approach to SD-WAN, as part of a healthy evolution of existing networks, is possible thanks to the emergence of new, next generation SD-WAN solutions. Simplified SD-WAN deployment, achieved through a single-box, multi-service approach, where SD-WAN, local infrastructure management and fully open VNFs are all built in, is an attractive and underserved model. Inhabiting this space will enable service providers to continue to deliver legacy services, while unlocking new revenues and empowering their enterprise customers to manage connectivity more efficiently and flexibly.

It's time to embrace the Internet of Things in manufacturing

What does manufacturing look like in 2021? Lukas Baur from TeamViewer explains how IoT plays a critical role in shaping the sector's future

Businesses of all shapes and sizes are facing up to the realisation that there is no going back to a pre-pandemic office. Despite some industries, like manufacturing, requiring on-the-ground staff, regulations and social distancing measures will continue to dominate factories and production lines for the foreseeable future. But this does not mean manufacturers cannot operate a seamless and efficient production line. Smart solutions such as IoT and AR sit at the heart of the sector's future, enabling manufacturers complete visibility into the health of its machines and visual based support, no matter the location of specialist technicians and engineers.

Manufacturers can use IoT solutions to fix issues in remote setups, increase operational efficiencies, as well as get total visibility into the status and performance of their machines with real-time insights around the health of the equipment. In turn, IoT offers three main benefits in a remote setup

Remote requirements

Remote working has not been a simple transition for manufacturers. Frontline staff of course cannot do their jobs from home, but according to research from Leesman, there are still 60% of manufacturing employees working remotely — a huge jump from just 26% pre-Covid. Furthermore, the bigger issue is that 53% of manufacturing workers have no experience working from home. This has led to heightened risks around a reduction in transfer knowledge and shared learning. In the long-term, a remote workforce could have serious consequences on the manufacturing sector, as machines risk not getting the maintenance and care required to run a seamless and efficient production line.

But manufacturers don't need to get stuck in this rut. Thanks to IoT & AR-led solutions such as remote access, predictive maintenance and AR-based instructions, manufacturers can maintain a remote workforce whilst also keeping their production lines up and running. These technologies have been emerging for some time, but the pandemic has turned them from desirable assets into business-critical components.

Enter IoT

Manufacturers can use IoT solutions to fix issues in remote setups, increase operational efficiencies, as well as get total visibility into the status and performance of their machines with real-time insights around the health of the equipment. In turn, IoT offers three main benefits in a remote setup:

Remote operations – manufacturers can control, monitor, and manage machine endpoints in the field from a remote location. It enables them to perform changes in a remote location and use real-time data to investigate an endpoint status without depending on on-site visits. This use of IoT also has huge financial benefits, an estimated $50 billion per annum according to Deloitte.

Remote assistance – thanks to IoT data, manufacturers can detect, diagnose and fix issues on IoT endpoints. This means manufacturers can address issues without depending on on-the-ground technical assistance or at least targeting technician deployment more effectively when needed.

Remote alarming – manufacturers can monitor and detect anomalies in IoT endpoint data, and define conditional rules that trigger subsequent actions when thresholds are met. This could include increasing revenue through setting up an alarm to stop excess/waste production or mitigating damage by alerting technicians of an error before downtime occurs.

Ultimately, embracing IoT solutions enable manufacturers to get a transparent view of their machine health whilst maintaining a remote workforce.

AR-based support – bridging the knowledge gap between experienced employees that might not be able to travel for on-site visits and less experienced workers on the field can be achieved with the help of AR. Technicians working remotely can guide their colleagues via AR-based support as they would be on the ground as well. Trainings or routine tasks on the other hand can be supported by AR-based workflows, helping frontline workers in the field to maintain a high quality of work even if the experts are not around.

Smart future

IoT and AR are not just a critical support in maintaining a remote workforce, but have a central role in the digital transformation of the manufacturing sector as they enable manufacturers to connect legacy systems, analogue equipment and their workers. Businesses can apply predictive analytics to all monitored machine and sensor data in real time, meaning manufacturers get real time information and full visibility about a machine's health. IoT, therefore, isn't just streamlining operations but enabling manufacturers to accelerate digitalisation through connecting all of its machines, smart or not.

Whilst there remain countless uncertainties about the future of work, IoT & AR can help manufacturers manage their production line no matter the challenges that lie ahead. Implementing remote operations, remote assistance, remote alarming through IoT and AR-based support, does not just support a remote working environment, but prepares manufacturers for a smarter future. ■

Top tips to keep your business 'always-on'

Michael Cade, senior global technologist, Veeam

Maintaining customer service standards has proven a really tough task for many businesses during the pandemic. But customers aren't going to stay around for long if service slips – they'll quickly start looking for alternatives if they don't feel what they're paying for lives up to their expectations.

It's a tricky thing to manage. The nature of modern business is that an effective IT strategy now has an impact on all kinds of other activities. Keeping systems protected and available provides the strongest platform for employees to perform at their best, and helps businesses stay as agile as possible. Here are four tips we've found particularly useful for businesses to bear in mind, in order to help them meet customer expectations and deliver great service, no matter the challenges in front of them.

1. Proactivity is key

The threat of cybercriminals and software bugs don't go away just because security has slipped on the priority list. Businesses should make sure they're investing in strong and reliable backup and disaster recovery solutions to proactively protect their data. An effective disaster recovery plan could be the difference between a successful business and a struggling one.

It all starts with an impact assessment – firms should be getting a clear understanding of where disaster recovery fits within their overall strategy. Identifying the apps and processes critical for maintaining consistent quality of service is highly useful. From there, setting things like ideal recovery targets is much more straightforward.

2. Invest in AI

Businesses are more successful when employees are given the space to focus on the most important tasks – especially those that are more creative and require more complex decision making and planning. The development of Artificial Intelligence (AI) and machine learning has the potential to change the way businesses work and lighten their load.

Administrative tasks currently take up significant amounts of time. Lengthy reporting processes and internal emails can crowd out the time that's needed for other activities that might add more value. AI software can thrive in these kinds of routine environments. The potential time savings could be immense too – analysis from McKinsey found the average professional spends 28% of the working day reading and answering emails. Optimising the workload for employees means that individuals can focus on the priority actions needed to meet customer demands.

3. Data is crucial for productivity

An increase in workload can be challenging but it should not result in surprises. Analysing data around productivity and customer interactions can help balance capacity and more effectively plan for employee absences. Organisations should encourage all departments to extend their IT ability, and start using the performance metrics they might already have at their disposal in smarter ways.

Becoming more data-driven allows businesses to ensure that productivity remains consistent even during crunch periods, and also that time is being invested in the right way. The ability to make informed decisions based on the very latest information can be hugely useful. Businesses produce huge amounts of data, but if there isn't a culture that understands the importance of it and takes its value seriously at a high level, it will remain more of a burden than an advantage.

4. Always backup

While urgent priorities can always crop up, teams with a reduced workforce shouldn't have any major issues if proper plans have been put in place. However, a team that doesn't backup their data is putting themselves at major risk. It seems obvious, but this data can often represent serious time and investment, as well as being the very foundation of a company's continued operation.

A progressive business takes safeguarding data seriously. It's not just a case of staying operational – it's also part of staying compliant with the likes of the General Data Protection Act (GDPR) and other data protection legislation. Putting reasonable measures in place to safeguard data is now a basic expectation of data controllers by the Information Commissioners' Office (ICO).

The Veeam 3-2-1 rule, which involves keeping three copies of data on two different media, with one offsite, has been a common rule of thumb for good reason. Having a robust Cloud Data Management strategy which includes automated backup solutions is crucial and provides the peace of mind that allows employees to focus on the things they do best.

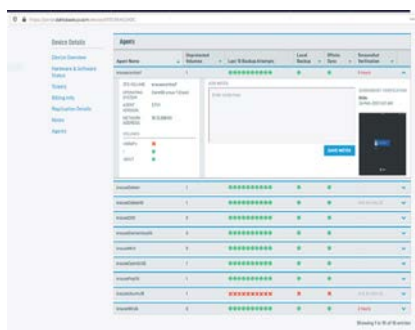
PRODUCTS

Citing a sharp increase in cyber incidents among its customers, **Daisy** says it is no coincidence that it has introduced a new product to its disaster recovery range. The company says most backup solutions do not have the coverage of its new product, called Acronis by Daisy. Among the features Daisy quotes are built in antivirus, anti-malware and ransomware protection; and backup, security and device management features which provide end-to-end backup, recovery and ransomware protection for all endpoints. These include mobiles and tablets, desktops and laptops, virtual machines and servers, and cloud productivity suites such as Microsoft 365 and Google Workspace. It says Acronis by Daisy, available in a choice of licence packs, eliminates complexity, delivers new security capabilities and keeps costs down. Daisy says that, in the fight against cybercrime, it recommends aligning business continuity and security functions to increase resilience And it says Acronis by Daisy, which incorporates technology from Acronis, makes it easier to protect and support homeworkers Increased homeworking, says the company, is providing new opportunities for cybercriminals and additional challenges for IT managers, so security solutions need to adapt, to help organisations keep things simple, secure and resilient. And Daisy warns of the damage data breaches can have. Quoting a study by Ponemon Institute for Emerson, it says the costs are: 25 per cent in system downtime; 25pc, theft of assets or information; 10pc damage to infrastructure; 30pc, loss of IT and end-user productivity; 8pc reputational damage (more if made public); and 4pc, lawsuits, fines and regulatory actions. Successful attacks, it says, cost large organisations £5.3m on average. *dcs.tech/acronis*

If disaster strikes your offices, move into ours, says **Sungard Availability Services**. It has set up workplace recovery sites throughout the UK – some alongside its data centres – including in Boreham-wood, Elland, Bristol, Coventry, Leicester, Crawley and Stockport. Each, says Sungard, has enterprise-grade kit and high-speed connectivity as well as amenities such as conference and rest areas. With a choice of three tiers of service, the company says each workplace can provide businesses with all of the IT equipment, PCs, and telephones they need, plus dealing room turrets. Facilities can be tailored to meet specific recovery times or compliance requirements. Each suite, says Sungard, is self-contained and can include dedicated meeting rooms and canteen areas. All buildings have hardened infrastructure with UPS and generators. With sites around the world, Sungard says it is able to offer alternative facilities in the event of even the most crippling widespread disasters. The company says that unlike other managed workplaces, it gives businesses full-time access to the space they need, with a robust and secure infrastructure. Sungard quotes recent research by IDC which says that more than three-quarters (77 per cent) of employees in the UK expect that a mixture of on-site and remote working will be commonplace. It says that as its workplaces are sited outside of major city hubs it means many employees will find that having to commute into a central city location via public transport will be a thing of the past, particularly post pandemic. Sungard Availability Services says it has 75 hardened data centres and workplace recovery facilities in nine countries. *sungardas.com*

In a time where digital dependency has rapidly accelerated, uptime and business continuity has never been more crucial, says **Schneider Electric**. The company points out that uninterruptible power supplies (UPS) provide power protection for data centres and mission-critical applications. To help safeguard businesses against downtime, the company recently added 250, 300, and 400 kVA 3-phase systems to its *Easy UPS 3L* range. Schneider says they offer simplified installation and streamlined configuration and are quick to deploy and easy to service. It says that -- with a compact footprint, highly available parallel and redundant design and robust electrical specifications -- the Easy UPS 3L range protects critical equipment in a wide range of operating conditions from damage due to power outages, surges and spikes. Easy UPS 3L models, it says, include a wide battery voltage window and accommodate a variety of battery configurations, with a range of options and accessories for optimum customisation and simplified integration into a number of IT environments. And Schneider says that UPS models offer resiliency against harsh environments with conformal-coated printed circuit boards -- a thin polymeric film to protect the PCB and its components -- replaceable dust filter, unity power factor and strong overload protection. These, it says, make them a reliable solution for business continuity, while reducing system complexity and cost. Schneider says that, with their versatile architecture, Easy UPS 3L models can be deployed in a parallel or N+1 configuration for increased redundancy and capacity. And it says customers can also benefit from the company's global service team with connections to a strong local network of power and electrical specialists. It says that the start-up service, for example, is included to ensure that the Easy UPS 3L is properly and safely configured for industry-leading reliability, safety and peace of mind. *se.com*

Companies can recover from a disaster in minutes with Siris, says **Datto**, which it describes as an all-in-one continuity and disaster recovery product. Siris, available for an all-inclusive monthly fee, uses what Datto calls inverse chain technology. This, it says, prevents the risk of file damage because the base image is always the newest file. It differs from traditional backups, says the company, where computers must rely on older files to restore newer ones. Datto says its technology ensures that the full image is always at the front of the backup chain and does not rely on past files for recovery. Siris, it says, prevents data loss and minimises downtime in the event of a disaster. It offers verified cloud and local backups, instant virtualization for fast system restoration, restore options for any scenario, screenshot and application backup verification and proactive ransomware detection. Additionally, it is backed by the Datto cloud with regional data centres across the world, and says that businesses have full control over their data sovereignty. Datto says updates to Siris are released as required, as frequently as bi-weekly or monthly. Two recent features include Agentless Backup which can back up any virtual machine on the VMWare hypervisor, giving customers the capability to protect edge devices, and integration with Datto Remote Monitoring & Management (RMM). This, it says, greatly improves efficiency by letting MSPs monitor their customers' entire BCDR (business continuity and disaster recovery) deployments directly from Datto's RMM. Datto was founded in Connecticut in 2007 and has locations around the world, including in Reading, Amersham and Richmond upon Thames. *datto.com*



Please meet...

Neil Hammerton, CEO & co-founder, Natterbox

What is the best thing about your job?

"Work is a huge part of almost all of our lives, yet many of us don't enjoy our job. In fact, according to research from 2019, 85% of us hate it. One of my missions is therefore to ensure that all of my colleagues at Natterbox feel happy and even excited at the thought of coming into work. No Sunday blues here!

"That's why we invest heavily in the wellbeing of our staff and the best thing about my job is seeing the benefits of our efforts.

"For example, we hired our Chief People Officer, Clare, to be available for a chat at any time of the day and ensure we always have someone on hand to make sure everyone's work/life balance, is indeed balanced. We also host amazing events such as our annual Summer Experience Day for charity. Last year this involved microlighting and quad biking among other incredible activities, all to show our support for a charitable cause, and to show Natterbox staff our thanks for all of the hard work they do year-round."

Who has been your biggest inspiration?

"I once I read a book by Richard Branson. In it, he said that anyone could master any business in just three months. And this was true for Natterbox – having had no knowledge of telecoms prior to founding the company, it took us about three months before we felt truly confident enough to have conversations with others in the industry.

"It's therefore to this one piece of advice and the inspiration from Richard Branson's own business success that I owe my confidence for taking that risk, which has now massively paid off."

What is your biggest regret?

"We all make mistakes through life and there are always things we could have done better. But to dwell is to not move forward. That's why my goal is to live life without regrets. We can't turn back the clock, but we always have control of our future."

If you had to work in a different industry, what would it be?

"One of my greatest passions outside of work is flying. If I hadn't taken the risk to work in the telecoms industry, I would have loved to have been in aviation. Dream job: helicopter pilot for Air Ambulance."

Who was your hero when you were growing up?

"One of my favourite films was Rocky, and the main character, played by Sylvester Stallone, was a hero of mine. One of my favourite quotes from the film is: "It's not how hard you can hit that counts but how hard you can get hit and still get back up.

"It's an idea I still like to live by today. For example, Natterbox experienced one of its biggest challenges in 2014, when the company was focusing all of its energy on compliant mobile voice recording, to align with the MIFID II reporting. MIFID II was an amended version of the Markets in Financial Instruments Directive, which was designed to offer greater protection for investors and inject more transparency into all asset classes.

"At the time, the market looked like it was raring to go with this European directive and we were in a great position – that is, until major banks lobbied governments to push MIFID II back by two years. We found ourselves having to completely re-focus the business trajectory towards the CRM telephony market.

"Growth stagnated for a while and the mobile voice recording arm of the business went from making up 60% of the revenue to representing only 10%. But the ability to get back up despite being hit ended up being a great move for the business. The change of focus to CRM telephony now accounts for the other 90% of our business."

The Beatles or the Rolling Stones?

"It has to be The Beatles!"

What would you do with £1m?

"Invest in Natterbox (and maybe buy a helicopter)! We are already helping our clients to navigate these challenging times. But there's so much more to be done in the world of telephony and CRM, especially as we settle into this new working from home era. We haven't even touched the surface!"

Which rival do you most admire?

"John Pendry. He was the World Champion for hang gliding when I started competition flying back in 1985. He is an inspiration and I never had any doubt in his ability to beat anyone!"

What's the weirdest question you've been asked at an interview?

"Beatles or Rolling stones!"

Which law would you change?

"The air law, which restricts low flying near man-made objects. Closely followed by the fact that it's unlawful to be drunk in a pub!"

"I once I read a book by Richard Branson. In it, he said that anyone could master any business in just three months"